Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (currently amended) A method of processing out-of-order messages, comprising:

determining a largest nonce value yet seen from a plurality of nonce values of out-of-order messages;

comparing a nonce value of a received out-of-order message with said largest nonce value yet seen;

comparing said nonce value to an acceptance window in response to said nonce value not exceeding said largest nonce value yet seen;

~~adjusting~~ increasing a size of a range of acceptable nonce values within said acceptance window, where ~~the~~ said size of said range is based on said largest nonce value yet seen; and

rejecting said received out-of-order message if ~~in response to~~ said nonce value ~~falling~~ falls outside said acceptance window.

2. (currently amended) The method according to claim 1, further comprising:

designating said nonce value as said largest nonce value yet seen ~~in response to~~ if said nonce value ~~exceeding~~ exceeds said largest nonce value yet seen.

3. (currently amended) The method according to claim 1, further comprising:

replacing said largest nonce value yet seen with said nonce value ~~in response to~~ if said nonce value ~~exceeding~~ exceeds said largest nonce value yet seen.

4. (currently amended) The method according to claim 1, further comprising:

~~adjusting~~ increasing ~~an~~ said acceptance window if ~~based on~~ said nonce value ~~exceeding~~ exceeds said largest nonce value yet seen.

5. (previously presented) The method according to claim 1, further comprising:

designating said received out-of-order message as a replay attack.

6. (currently amended) The method according to claim 1, further comprising:

comparing said nonce value to a window mask value if ~~in response to~~ said nonce value ~~falling~~ falls within said acceptance window; and

rejecting said received out-of-order message if ~~in response to an outcome of said comparison of~~ said nonce value is within ~~to~~ said window mask value ~~being true~~.

7. (previously presented) The method according to claim 6, further comprising:

designating said received out-of-order message as part of a replay attack.

8. (currently amended) The method according to claim 1, further comprising:

comparing said nonce value to a window mask value if ~~in response to~~ said nonce value ~~falling~~ falls within said acceptance window; and

accepting said received out-of-order message if ~~in response to an outcome of said comparison of~~ said nonce value is outside ~~to~~ said window mask value ~~being false~~.

9. (previously presented) The method according to claim 8, further comprising:

designating said nonce value as a largest nonce value yet seen.

10. (currently amended) An apparatus for processing out-of-order messages, said apparatus comprising:

a communication interface configured to transmit and receive a plurality of packets; and

a controller, wherein said controller is configured to:

determine a largest nonce value yet seen from a plurality of nonce values of out-of-order messages;

compare a nonce value of a received out-of-order message and said largest nonce value yet seen;

compare said nonce value to an acceptance window in response to said nonce value not exceeding said largest nonce value yet seen;

~~adjust~~ increase a size of a range of acceptable nonce values within said acceptance window, where ~~the~~ said size of said range is based on said largest nonce value yet seen; and

reject said received out-of-order message if ~~in response to~~ said nonce value ~~falling~~ falls outside said acceptance window.

11. (currently amended) The apparatus according to claim 10, wherein:

said controller is further configured to designate said nonce value as said largest nonce value yet seen if ~~in response to~~ said nonce value ~~exceeding~~ exceeds said largest nonce value yet seen.

12. (currently amended) The apparatus according to claim 10, wherein:

said controller is further configured to ~~adjust~~ increase an acceptance window if ~~in response to~~ said largest nonce value yet seen ~~in response to said nonce value exceeding~~ exceeds said largest nonce value yet seen.

13. (currently amended) The apparatus according to claim 10, wherein:

said controller is further configured to replace said largest nonce value yet seen with said nonce value if ~~in response to~~ said nonce value ~~exceeding~~ exceeds said largest nonce value yet seen.

14. (previously presented) The apparatus according to claim 10, wherein:

said controller is further configured to designate said received out-of-order message as part of a replay attack.

15. (currently amended) The apparatus according to claim 10, wherein said controller is further configured to:

compare said nonce value to a window mask value if ~~in response to~~ said nonce value ~~falling~~ falls within said acceptance window; and

reject said received out-of-order message if said nonce value falls outside said acceptance window ~~in response to an outcome of said comparison of said nonce value to said window mask value being true~~.

16. (previously presented) The apparatus according to claim 15, wherein:

said controller is further configured to designate said received out-of-order message as part of a replay attack.

17. (currently amended) The apparatus according to claim 10, wherein said controller is configured to:

compare said nonce value to an acceptance window ~~window mask~~ value if ~~in response to~~ said nonce value ~~falling~~ falls within said acceptance window; and

accept said received out-of-order message if said nonce value falls within said acceptance window ~~in response to an outcome of said comparing of said nonce value to said window mask value being false~~.

18. (previously presented) The apparatus according to claim 17, wherein:

said controller is further configured to mark said nonce value as said largest nonce value yet seen.

19. (currently amended) A computer readable storage medium on which is embedded one or more computer programs, said one or more computer programs implementing a method of processing out-of-order messages, said one or more computer programs comprising a set of instructions for:

determining a largest nonce value yet seen from a plurality of nonce values of out-of-order messages;

comparing a nonce value of a received out-of-order message and said largest nonce value yet seen;

comparing said nonce value to an acceptance window in response to said nonce value not exceeding said largest nonce value yet seen;

~~adjusting~~ increasing a size of a range of acceptable nonce values within said acceptance window, where ~~the~~ said size of said range is based on said largest nonce value yet seen; and

rejecting said received out-of-order message if ~~in response to~~ said nonce value not ~~falling~~ falls within said acceptance window.

20. (currently amended) The computer readable storage medium in according to claim 19, said one or more computer programs further comprising a set of instructions for:

designating said nonce value as said largest nonce value yet seen if ~~in response to~~ said nonce value ~~exceeding~~ exceeds said largest nonce value yet seen.

21. (currently amended) The computer readable storage medium in according to claim 19, said one or more computer programs further comprising a set of instructions for:

replacing said largest nonce value yet seen with said nonce value if ~~in response to~~ said nonce value ~~exceeding~~ exceeds said largest nonce value yet seen.

22. (currently amended) The computer readable storage medium in according to claim 19, said one or more computer programs further comprising a set of instructions for:

~~adjusting~~ increasing an acceptance window based on said nonce value if ~~in response to~~ said nonce value ~~exceeding~~ exceeds said largest nonce value yet seen.

23. (previously presented) The computer readable storage medium in according to claim 19, said one or more computer programs further comprising a set of instructions for:

designating said received out-of-order message as a replay attack.

24. (currently amended) The computer readable storage medium in according to claim 19, said one or more computer programs further comprising a set of instructions for:

comparing said nonce value to a window mask value if ~~in response to~~ said nonce value ~~falling~~ falls within said acceptance window; and

rejecting said received out-of-order message if said nonce value falls outside said acceptance window ~~in response to an outcome of said comparison of said nonce value to said window mask value being true~~.

25. (previously presented) The computer readable storage medium in according to claim 24, said one or more computer programs further comprising a set of instructions for:

designating said received out-of-order message as part of a replay attack.

26. (currently amended) The computer readable storage medium in according to claim 19, said one or more computer programs further comprising a set of instructions for:

comparing said nonce value to a window mask value if ~~in response to~~ said nonce value ~~falling~~ falls within said acceptance window; and

accepting said received out-of-order message if said nonce value falls within said acceptance window ~~in response to an outcome of said comparing of said nonce value to said window mask value being false~~.

27. (previously presented) The computer readable storage medium in according to claim 26, said one or more computer programs further comprising a set of instructions for:

designating said nonce value as said largest nonce value yet seen.

28. (currently amended) A system for processing out-of-order messages in a peer-to-peer configuration, comprising:

a first peer configured to provide secure communication;

a second peer configured to provide said secure communication; and

a secure communication module configured to be executed by said first peer and second peer, wherein said secure communication module is configured to:

determine a largest nonce value yet seen from a plurality of nonce values of a out-of-order messages;

compare a nonce value to a filter in response to said nonce value of a received out-of-order packet not exceeding said largest nonce value yet seen;

compare said nonce value to a replay mask;

~~adjust~~ increase a size of a range of acceptable nonce values within said acceptance window, where ~~the~~ said size of said range is based on said largest nonce value yet seen; and

accept said received out-of-order packet if said nonce value falls within said replay mask ~~in response to said comparison of said nonce value and said replay mask being false~~.

29. (currently amended) The system according to claim 28, wherein:

said secure communication module is further configured to designate said nonce value as said largest nonce value yet seen if ~~in response to~~ said nonce value ~~exceeding~~ exceeds said largest nonce value yet seen.

30. (currently amended) The system according to claim 28, wherein:

said secure communication module is further configured to ~~adjust~~ increase said filter based on said largest nonce value yet seen if ~~in response to~~ said nonce value ~~exceeding~~ exceeds said largest nonce value yet seen.

31. (currently amended) The system according to claim 28, wherein:

said secure communication module is further configured to reject said received out-of-order packet if ~~in response to~~ said nonce value falls ~~falling~~ outside said filter.

32. (previously presented) The system according to claim 31, wherein:

said secure communication module is further configured to designate said received out-of-order packet as part of a replay attack.

33. (currently amended) The system according to claim 32, wherein:

said secure communication module is further configured to reject said received out-of-order packet if ~~in response to said comparison of~~ said nonce value ~~and~~ falls outside said replay mask ~~being true~~.

34. (previously presented) The system according to claim 33, wherein:

said secure communication module is further configured to designate said received out-of-order packet as part of a replay attack.

35. (currently amended) The system according to claim 28, wherein:

said secure communication module is further configured to reject said received out-of-order packet if ~~in response to~~ said nonce value ~~fails to fall~~ falls outside ~~within~~ said filter; and

said secure communication module is further configured to designate said received out-of-order packet as part of a replay attack.

36. (currently amended) An interceptor device for processing out-of-order messages, said interceptor device comprising:

a network interface;

an expected sequence register configured to enumerate an expected sequence number of a packet received out-of-order from a second network device;

a memory configured to store a replay mask; and

a controller, wherein said controller is configured to:

determine a largest nonce value yet seen from a plurality of nonce values of out-of-order messages;

compare a nonce value to a filter in response to a sequence number of a received out-of-order packet via said network interface does not exceed said largest nonce value yet seen retrieved from said expected sequence register;

compare said sequence number to said replay mask retrieved from said memory;

~~adjust~~ increase a size of a range of acceptable nonce values within said replay mask ~~acceptance window~~, where ~~the~~ said size of said range is based on said largest nonce value yet seen; and

accept said received out-of-order packet if ~~in response to said comparison of~~ said sequence number ~~and~~ falls within said replay mask ~~is false~~.

37. (currently amended) The interceptor device according to claim 36, wherein:

said controller is further configured to designate said sequence number as said largest nonce value yet seen if ~~in response to~~ said sequence number ~~exceeding~~ exceeds said largest sequence number yet seen.

38. (currently amended) The interceptor device according to claim 36, wherein:

said controller is further configured to ~~adjust~~ increase said filter based on said largest nonce value yet seen if ~~in response to~~ said sequence number ~~exceeding~~ exceeds said largest nonce value yet seen.

39. (currently amended) The interceptor device according to claim 36, wherein:

said controller is further configured to reject said received out-of-order packet if ~~in response to~~ said sequence number falls ~~falling~~ outside said filter.

40. (previously presented) The interceptor device according to claim 36, wherein:

said controller is further configured to designate said received out-of-order packet as part of a replay attack.

41. (currently amended) The interceptor device according to claim 36, wherein:

said controller is further configured to reject said received out-of-order packet if ~~in response to said comparison of~~ said sequence number falls outside ~~and~~ said replay mask ~~being true~~.

42. (previously presented) The interceptor device according to claim 41, wherein:

said controller is further configured to designate said received out-of-order packet as part of a replay attack.

43. (currently amended) The interceptor device according to claim 36, wherein:

said controller is further configured to reject said received out-of-order packet if ~~in response to~~ said sequence number falls ~~falling~~ outside said filter; and

said controller is further configured to designate said received out-of-order packet as part of a replay attack.